FIREEYE | MANDIANT

DEPLOYMENT & INTEGRATION SERVICES DATA SHEET

Helix

BENEFITS

- **Efficient deployment** by FireEye experts using best-practice configurations
- **Maximum visibility** via seamless onboarding of FireEye and third-party cloud and on-premise data sources
- **Use case implementation** with guidance on data source selection, custom rule development and threat hunting enablement
- **Operational readiness** facilitated by hands-on knowledge transfer to enable rapid identification, triage and containment of security events

Overview

FireEye Deployment and Integration Services enable you to seamlessly integrate FireEye Helix into your security operations to bring world-class threat intelligence and analytics into any security stack. These services help you install, configure and onboard a variety of security products, including physical or virtual on-premise sensors, endpoint agents, cloud-based solutions, and threat intelligence sources. Our security experts implement Helix to quickly connect and enhance all your security solutions so your team can start surfacing unseen threats and making expert decisions based on frontline intelligence. We offer three types of services to help you maximize the value of your investment in FireEye Helix:

- Deployment Jumpstart Services
- Deployment of Helix for Managed Defense
- Helix Health Check and Tuning

Deployment Jumpstart Services

Jumpstart Services for FireEye Helix are designed to help you quickly start using FireEye threat intelligence and analytics by onboarding available data sources into Helix, configuring dashboards and rules to implement desired use cases, and showing your team how to effectively use Helix. Each deployment starts with a Helix Planning Workshop to identify and prioritize data sources to be ingested and to review use cases for those data sources to plan out rules, widgets and dashboards for implementation. Using workshop data, FireEye experts set up network sensors, onboard on-premise and cloud data sources, develop parsers as needed and implement the identified use cases. During the console build out and customization phase, these experts discuss the use and management of Helix with your Helix system administrators and security analysts.

Helix Deployment Jumpstart Services include:

- Architecture design review and planning for FireEye Helix
- Configuration and setup based on FireEye best practices
- Connection to Mandiant Threat Intelligence and content updates
- Deployment of network sensors (as applicable)
- Onboarding of FireEye and third-party data sources (on-premise and cloud)
- Review of onboarded data sources to verify expected visibility into network and host events
- Configuration and review of rules, lists, and dashboards
- Review of FireEye Helix for analysts and administrators
- Introduction to FireEye customer resources such as the FireEye Customer Support Portal and Community and FireEye Market

Supplemental services for the development of custom Helix Connect modules and custom parsers can be added to a Helix jumpstart.

Deployment of Helix for Managed Defense
FireEye Helix can be quickly and effectively deployed to help power Mandiant Managed Defense. FireEye experts can work with you to identify and prioritize available data sources based on Managed Defense use cases for alerting on and investigating suspicious activity in your network. Based on the prioritized list of data sources, the experts set up network sensors and onboard the applicable on-premise and cloud data sources. They then review the ingested data to ensure it provides the necessary visibility for Managed Defense and implement rules and use cases.

Helix for Managed Defense Deployment services include:

- Architecture design review and planning for FireEye Helix
- Configuration and setup based on FireEye best practices
- Connection to Mandiant Threat Intelligence and content updates
- Deployment of network sensors (as applicable),
- Onboarding of FireEye and third-party data sources (on-premise and cloud), as prioritized for Managed Defense use cases
- Review of onboarded data sources to verify expected visibility into network and host events
- Configuration and review of rules, lists and dashboards for Managed Defense use cases
- Introduction to FireEye customer resources such as the FireEye Customer Support Portal and Community and FireEye Market

Helix Health Check and Tuning
With the frequent changes that occur in most corporate networks and the rapid pace of innovation in the FireEye Helix solution, it can be challenging to ensure your security solutions maintain the level of visibility and protection you expect. To get the most coverage and value from FireEye Helix, the Health Check and Tuning service reviews the operation and configuration of your FireEye Helix deployment and provides recommendations for data sources and use cases that align with your security goals and FireEye best practices.

The Helix Health Check and Tuning service includes:

- Comprehensive assessment of system health and performance
- Review of existing data sources and comparison to FireEye and Mandiant recommendations
- Optimization recommendations and tuning for noisy data sources
- Review of network architecture regarding placement of network sensors, if applicable
- Explanation and enablement of new features, capabilities, and modules
- Assessment of ruleset coverage based on available data sources
- Analysis of dashboards and rules in meeting desired use cases
- Review of FireEye Helix usage for analysts

Table 1. Helix Services Comparison.*

	Basic Jumpstart	Advanced Jumpstart	Helix for MD	Health Check and Tuning
Helix planning workshop	✓	✓	MD focused	
Deployment and configuration of network sensors and evidence collectors	Up to 2	Up to 5	Up to 2	Review
Onboarding of on-premise data sources and configuration of Helix Connect modules to ingest cloud data sources	Up to 4 data sources	Up to 10 data sources	Up to 4 data sources	Review
Development of custom Helix Connect module, if applicable	Add-on service*	Add-on service*		
Connection to Mandiant Threat Intelligence	✓	✓	✓	Review
Review of onboarded data sources to verify expected visibility	✓	✓	✓	Review
Development of custom parsers, if applicable	Add-on service*	Add-on service*		
Customization of included rules and dashboards		✓		Review
Development of custom rules, widgets, and dashboards		✓		Review
Onboarding with Mandiant Managed Defense (if applicable)	✓	✓	✓	Review
Review of data source onboarding and management best practices	✓	✓	✓	✓
Analyst knowledge transfer (alert review and triage)	✓	✓		✓
Assessment of system health and performance	✓	✓	✓	✓
Documentation of installed solution	✓	✓	✓	✓
Assessment of ruleset coverage based on available data sources	✓	✓	✓	✓
Guidance on API and custom integrations		✓		✓

*Supplemental services can be purchased for the development of custom Helix Connect modules and parsers.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.
At FireEye, our mission is to relentlessly protect organizations with innovative technology, intelligence and expertise gained on the frontlines of cyber attacks. Learn how at www.FireEye.com.

About Mandiant Solutions
Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.